ANNEX A: INFORMATION REQUIRED FOR ALL WORK UNITS (EAL4)

This annex provides a summary of the information that must be reported in the ETR for each work unit in order to support the assignment of a **pass** verdict for the corresponding evaluator action.

It should be noted that this Annex is to be used as a supplement, in conjunction with the CEM. The Annex documents the minimum level of justification required in an ETR. Where the claims made for the TOE include factors such as a requirement being met in a novel or complex way, or if the TOE is complex, there may be a need for additional explanation to support the assigned verdict beyond that documented in this Annex. ***Therefore as appropriate, a validator may request additional evidence to support a verdict justification.***

The CC allows great latitude in the organization of evaluation evidence. This means that the design documents required by the CC may be comprised of sections extracted from one or more documents. The document references in the ETR should identify both the document and the sections within the document that apply to a work unit. If the required information was found in more than one section of a document, all sections must be identified. Overly broad references should not be used (e.g., If only one page of a 20-page section is applicable, then a general reference to the entire section is unacceptable. Rather, there must be a reference to the relevant page or paragraphs within the section.). CCEVS requires that a minimum of 50 percent of the referenced material must be applicable to the work unit. Even finer granularity (i.e., 100 percent of the referenced material pertains to the work unit) will expedite the validation. This finer granularity will provide the validator with confidence that the evaluators looked at the actual evidence that was necessary to perform the work unit. Validators may request a review of documents that are referenced in the ETR, with the justification for review of the documents being the fact that the ETR references them.

The goal of this annex is to provide information (in addition to the CEM) to the evaluator so that a work unit report will add value to the ETR and thereby demonstrate understanding of the evidence examined. Implementation of the ETR template and the requirements of this Annex will result in a consistent evaluation documentation approach across CCTLs and will allow for consistency in validation activities. It should be noted that the following neither adds value to an ETR, nor demonstrates understanding:

1. Use of "stock phrases" from the CEM, or repeating the work unit (e.g., "the evaluator examined…" or "the evaluator checked…"); or

2. Repetition of information from the evidence examined, or

3. Vague work descriptions (e.g., "the evaluator performed a mental mapping").

The Annex is divided into the following groupings: PP Evaluation, ST Evaluation, and EAL 4 evaluation.

The overall goal of an ETR is to document evaluation results in a manner that allows the reader to gain confidence that the evaluation analysis was technically sound. This document provides information on how to document useful evaluation results. However, CCEVS reserves the right to provide additional clarification and guidance as needed.

The work units use the following categories to describe the ETR requirements.

A) Reference - Minimal description of simple methodologies, due to the trivial nature of work unit or the use of explicit CEM methodology for the work unit. This category would apply when one or more documents must be examined. This category may be used whenever the actual work was done under a different work unit. When this case applies, the "actual" work unit must be identified.

B) Elaborated Reference - Used when methodologies involve checklists that are created by the evaluator (e.g., requirement traceability matrices). A high level description of the methodology as it applies to the TOE must be presented. All completed checklists must be included in the ETR.

C) Analysis - Used for more complex methodologies. A detailed description of the methodology as it applies to the TOE under evaluation must be presented. This description should include the evaluation team's procedures used in carrying out the methodology on the TOE and its evidence. The evaluators must produce a detailed work log of the procedure's application. All procedures and logs must be included in the ETR.

PP AND ST EVALUATION

APE_DES.1—Evaluation of TOE Description

Work Unit	Category	Discussion
APE_DES.1-1	B	Explain why the description of the product or system type is sufficient.
APE_DES.1-2	B	Explain why the description of the IT features of the TOE in general terms is sufficient.
APE_DES.1-3	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
APE_DES.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
APE_DES.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

APE_ENV.1—Evaluation of security environment

Work Unit	Category	Discussion
APE_ENV.1-1	B	Elaborate on the choice of assumptions and why the description is sufficient.
APE_ ENV.1-2	B	Elaborate on the choice of threats and why the description is sufficient.
APE_ ENV.1-3	B	Elaborate on the choice of OSPs and why the description is sufficient.
APE_ ENV.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
APE_ ENV.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

APE_INT.1—Evaluation of PP introduction

Work Unit	Category	Discussion
APE_INT.1-1	A	Provide a reference to the exact location in the document.
APE_ INT.1-2	A	Provide a reference to the exact location in the document.
APE_ INT.1-3	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
APE_ INT.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
APE_ INT.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

APE_OBJ.1—Evaluation of security objectives

Work Unit	Category	Discussion
APE_OBJ.1-1	B	Document specific reference to points where the information is located (for TOE, environment, or both … could be multiple).
APE_OBJ.1-2	C	Include a tracing matrix with all threats, OSP, and TOE objectives covered. If such a matrix is already present in the PP, provide a reference to its location, including justification about the correctness of the matrix.
APE_OBJ.1-3	C	Include a tracing matrix with all threats, OSP, and objectives for the environment covered and trace assumptions to objectives. If such a matrix is already present in the PP, provide a reference to its location, including justification about the correctness of the matrix.
APE_OBJ.1-4	C	Explain why the justification (that the security objectives are suitable to counter each threat) provided in the PP is appropriate.
APE_OBJ.1-5	C	Explain why the justification (that the security objectives are suitable to cover each organizational security policy) provided in the PP is appropriate.
APE_OBJ.1-6	C	Explain why the justification (that the security objectives for the environment are suitable to cover each assumption) provided in the PP is appropriate.
APE_OBJ.1-7	C	Identify the salient characteristics of the evidence that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
APE_OBJ.1-8	C	Based upon the findings of APE_OBJ.1-4 through 1-6, completeness should be determined by ensuring that all threats, policies, and assumptions are addressed by the security objectives. Document results.
APE_OBJ.1-9	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

APE_REQ.1—Evaluation of IT security requirements

Work Unit	Category	Discussion
APE_REQ.1-1	A	Confirm that the TOE security functional requirements were drawn from CC Part 2.
APE_REQ.1-2	B	Explain the process used to check that each reference to a TOE security functional requirement component is correct.
APE_REQ.1-3	B	Explain the process used to check that the Part 2 components were correctly reproduced.
APE_REQ.1-4	A	Confirm that the TOE security assurance requirements were drawn from CC Part 3.
APE_REQ.1-5	B	Explain the process used to check that each reference to a TOE security assurance requirement component is correct.
APE_REQ.1-6	B	Explain the process used to check that the CC Part 3 components were correctly reproduced.
APE_REQ.1-7	B	Provide rationale as to why the justification to include / exclude EAL was appropriate.
APE_REQ.1-8	C	Document the analysis to determine that the rationale proves the assurance requirements selected are sufficient for the TOE and justifies the choice of EAL for the TOE.
APE_REQ.1-9	B	Explain the process used to determine whether there are requirements for the IT environment and, if so, whether they were identified as such.
APE_REQ.1-10	B	Explain the process used to determine whether all operations are identified in each component that has one or more operations. Identify all completed operations.
APE_REQ.1-11	B	Elaborate on the correctness of the component operations. Justify that the operation and any associated application notes were followed in all cases.
APE_REQ.1-12	B	Identify and list all uncompleted operations.
APE_REQ.1-13	A	Confirm that the rationale provides reasons for inclusion of all dependencies. If a dependency has been excluded, confirm that the rationale for exclusion is present.
APE_REQ.1-14	C	Document analysis to determine if it is appropriate that dependencies are not satisfied.
APE_REQ.1-15	A	Report whether an SOF level exists and whether it is one of the 3 valid levels.
APE_REQ.1-16	B	Elaborate on why the SOF-level is appropriate
APE_REQ.1-17	C	Identify the salient characteristics of the SOF claim and security objectives that were compared for consistency, using details on expertise, resources, and motivation, and document rationale as to why the selected characteristics are sufficient.
APE_REQ.1-18	A	Confirm that the security requirements rationale contains a tracing from TOE security requirements to objectives for the TOE.
APE_REQ.1-19	A	Confirm that the security requirements rationale contains a tracing from security requirements for the IT environment to security objectives for the environment.
APE_REQ.1-20	C	Analyze and justify the correctness of the tracing identified in APE_REQ.1-18.
APE_REQ.1-21	C	Analyze and justify the correctness of the tracing identified in APE_REQ.1-19.
APE_REQ.1-22	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
APE_REQ.1-23	C	Identify the characteristics of the IT security requirements that were compared and provide rationale as to why the selected characteristics are

		sufficient to work together to form a mutually supportive whole.
APE_REQ.1-24	B	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
APE_REQ.1-25	B	Identify the salient characteristics of the evidence/TOE that were compared for completeness and provide rationale as to why the selected characteristics are sufficient.
APE_REQ.1-26	B	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

APE_SRE.1—Evaluation of explicitly stated IT security requirements

Work Unit	Category	Discussion
APE_SRE.1-1	B	Explain the process used to check that the statement of the IT security requirements identifies all TOE security requirements that are explicitly stated without reference to the CC.
APE_SRE.1-2	B	Explain the process used to check that the statement of the IT security requirements identifies all security requirements for the IT environment that are explicitly stated without reference to the CC.
APE_SRE.1-3	B	Analyze and justify the appropriateness of the security requirements rationale.
APE_SRE.1-4	A	Confirm that the SRE form and format follows the CC.
APE_SRE.1-5	C	Document how the determination was made that each functional requirement was testable and traceable through the appropriate TSF representation. Document how the determination was made that each assurance requirement avoids the need for subjective evaluator judgment.
APE_SRE.1-6	B	Document how each requirement was determined to be clear and unambiguous.
APE_SRE.1-7	C	Analyze and justify how the security requirements rationale demonstrates that the assurance requirements are applicable and appropriate to support any explicitly stated TOE security functional requirements.
APE_SRE.1-8	C	Document analysis to determine that all dependencies have been identified for each SRE.

ST EVALUATION

ASE_DES.1—Evaluation of TOE description

Work Unit	Category	Discussion
ASE_DES.1-1	B	Explain why the description of the product or system type is sufficient.
ASE_DES.1-2	B	Explain why the description of the physical scope and boundaries of the TOE is sufficient.
ASE_DES.1-3	B	Explain why the description of the logical scope and boundaries of the TOE is sufficient.
ASE_DES.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
ASE_DES.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
ASE_DES.1-6	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics

		are sufficient.

ASE_ENV.1—Evaluation of security environment

Work Unit	Category	Discussion
ASE_ENV.1-1	B	Elaborate on the choice of assumptions and document why the description is sufficient.
ASE_ ENV.1-2	B	Elaborate on the choice of threats and document why the description is sufficient.
ASE_ ENV.1-3	B	Elaborate on the choice of OSPs and document why the description is sufficient.
ASE_ ENV.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
ASE_ ENV.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

ASE_INT.1—Evaluation of ST Introduction

Work Unit	Category	Discussion
ASE_INT.1-1	A	Identify the exact location of the ST identification information in the document.
ASE_ INT.1-2	A	Identify the exact location of the ST overview in the document.
ASE_ INT.1-3	A	Identify the exact location of the CC conformance claim in the document.
ASE_ INT.1-4	C	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient. What was reviewed to determine coherency.
ASE_INT.1-5	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
ASE_ INT.1-6	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

ASE_OBJ.1—Evaluation of security objectives

Work Unit	Category	Discussion
ASE_OBJ.1-1	B	Document the specific reference to points where the information is located (for TOE, environment, or both … could be multiple).
ASE_ OBJ.1-2	C	Include a tracing matrix with all threats, OSP, and TOE objectives covered. If such a matrix is already present in the ST, provide a reference to its location, including justification about the correctness of the matrix.
ASE_ OBJ.1-3	C	Include a matrix that traces all objectives for the TOE's environment to threats, OSPs, and assumptions. If such a matrix is already present in the ST, provide a reference to its location, including justification about the correctness of the matrix.
ASE_ OBJ.1-4	C	Explain why the justification (that the security objectives are suitable to counter each threat) provided in the ST is appropriate.
ASE_ OBJ.1-5	C	Explain why the justification (that the security objectives are suitable to cover each organizational security policy) provided in the ST is appropriate.
ASE_ OBJ.1-6	C	Explain why the justification (that the security objectives for the environment are suitable to cover each assumption) provided in the PP is appropriate.
ASE_ OBJ.1-7	C	Identify the salient characteristics of the evidence/TOE that were compared

		for coherency and provide rationale as to why the selected characteristics are sufficient.
ASE_ OBJ.1-8	C	Based upon the findings of ASE_OBJ.1-4 through 1-6, completeness should be determined by ensuring that all threats, policies, and assumptions are addressed by the security objectives. Document results.
ASE_ OBJ.1-9	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

ASE_PPC.1—Evaluation of PP claims

Work Unit	Category	Discussion
ASE_PPC.1-1	A	Document the reference to the exact location in the ST.
ASE_PPC.1-2	A	Document the reference to the location in the ST where each PP claim identifies the IT security requirements statements that satisfy the permitted operations of the PP or otherwise further qualify the PP requirements.
ASE_PPC.1-3	A	Document the reference to the location in the ST where each PP claim identifies those security objectives and IT security requirements that are additional to the security objectives and the IT security requirements contained in the PP.
ASE_PPC.1-4	C	Elaborate on completed operations that were performed on the IT security requirements from the PP, justifying why they are within the bounds set by the PP.

ASE_REQ.1—Evaluation of IT security requirements

Work Unit	Category	Discussion
ASE_REQ.1-1	A	Confirm that the TOE security functional requirements were drawn from CC Part 2.
ASE_REQ.1-2	B	Explain the process used to check that each reference to a TOE security functional requirement component is correct.
ASE_REQ.1-3	B	Explain the process used to check that the Part 2 components were correctly reproduced.
ASE_REQ.1-4	A	Confirm that the TOE security assurance requirements were drawn from CC Part 3.
ASE_REQ.1-5	B	Explain the process used to check that each reference to a TOE security assurance requirement component is correct.
ASE_REQ.1-6	B	Explain the process used to check that the CC Part 3 components were correctly reproduced.
ASE_REQ.1-7	B	Provide rationale as to why the justification to include / exclude EAL was appropriate.
ASE_REQ.1-8	C	Document analysis to determine that the rationale proves the assurance requirements selected are sufficient for the TOE and justifies the choice of EAL for the TOE.
ASE_REQ.1-9	B	Explain the process used to determine whether there are requirements for the IT environment and, if so, whether they were identified as such.
ASE_REQ.1-10	B	Explain the process used to determine whether all operations are identified in each component that has one or more operations. Identify all completed operations.
ASE_REQ.1-11	A	Explain the process used to check that all assignment and selection operations are performed.
ASE_REQ.1-12	B	Elaborate on the correctness of the component operations. Justify that the operation and any associated application notes were followed in all cases.
ASE_REQ.1-13	A	Confirm that the rationale provides reasons for inclusion of all dependencies. If a dependency has been excluded, confirm that the rationale for exclusion

		is present.
ASE_REQ.1-14	C	Document analysis to determine if it is appropriate that dependencies are not satisfied.
ASE_REQ.1-15	A	Report whether an SOF level exists and whether it is one of the 3 valid levels.
ASE_REQ.1-16	B	Elaborate on why SOF-level is appropriate.
ASE_REQ.1-17	C	Identify the salient characteristics of the SOF claim and security objectives that were compared for consistency, using details on expertise, resources, and motivation, and document rationale as to why the selected characteristics are sufficient.
ASE_REQ.1-18	A	Confirm that the security requirements rationale contains a tracing from TOE security requirements to objectives for the TOE.
ASE_REQ.1-19	A	Confirm that the security requirements rationale contains a tracing from security requirements for the IT environment to security objectives for the environment.
ASE_REQ.1-20	C	Analyze and justify the correctness of the tracing identified in ASE_REQ.1-18.
ASE_REQ.1-21	C	Analyze and justify the correctness of the tracing identified in ASE_REQ.1-19.
ASE_REQ.1-22	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
ASE_REQ.1-23	C	Identify the characteristics of the IT security requirements that were compared and provide rationale as to why the selected characteristics are sufficient to work together to form a mutually supportive whole.
ASE_REQ.1-24	B	Identify the salient characteristics of the evidence/TOE that were compared for coherency and provide rationale as to why the selected characteristics are sufficient.
ASE_REQ.1-25	B	Identify the salient characteristics of the evidence/TOE that were compared for completeness and provide rationale as to why the selected characteristics are sufficient.
ASE_REQ.1-26	B	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

ASE_SRE.1—Evaluation of explicitly stated IT security requirements

Work Unit	Category	Discussion
ASE_SRE.1-1	B	Explain the process used to check that the statement of the IT security requirements identifies all TOE security requirements that are explicitly stated without reference to the CC.
ASE_SRE.1-2	B	Explain the process used to check that the statement of the IT security requirements identifies all the security requirements for the IT environment that are explicitly stated without reference to the CC.
ASE_SRE.1-3	B	Analyze and justify the appropriateness of the security requirements rationale.
ASE_SRE.1-4	A	Confirm that the SRE form and format follows the CC.
ASE_SRE.1-5	C	Document how the determination was made that each functional requirement was testable and traceable through the appropriate TSF representation. Document how the determination was made that each assurance requirement avoids the need for subjective evaluator judgment.
ASE_SRE.1-6	B	Document how each requirement was determined to be clear and unambiguous.
ASE_SRE.1-7	C	Analyze and justify how the security requirements rationale demonstrates that the assurance requirements are applicable and appropriate to support any

		explicitly stated TOE security functional requirements.
ASE_SRE.1-8	C	Document analysis to determine that all dependencies have been identified for each SRE.

ASE_TSS.1—Evaluation of TOE summary specifications

Work Unit	Category	Discussion
ASE_TSS.1-1	B	Elaborate on whether assurance measures are included or pointed to in multiple references.
ASE_TSS.1-2	A	Confirm that the TSS contains a tracing from each IT security requirement to at least one TOE security functional requirement.
ASE_TSS.1-3	B	Justify why the level of detail was appropriate.
ASE_TSS.1-4	B	The tracing analysis should identify all references to security mechanisms in the ST, indicate with what security functions the mechanisms are associated, and how the mechanisms are associated with the security functions.
ASE_TSS.1-5	B	Analyze and justify the appropriateness of the TSS rationale for each TOE SFR.
ASE_TSS.1-6	C	Identify the salient characteristics of the SOF claims for the IT security functions and TOE security functional requirements that were compared for consistency, using details on expertise, resources, and motivation, and document rationale as to why the selected characteristics are sufficient.
ASE_TSS.1-7	C	Document analysis to assess the impact of additional information included in the IT security functions to determine that the inclusions of such information introduces no potential security weaknesses.
ASE_TSS.1-8	A	Confirm that the TSS contains a tracing from each assurance measure to at least one TOE security assurance requirement.
ASE_TSS.1-9	B	Analyze and justify the appropriateness of the TSS rationale for each TOE security assurance requirement.
ASE_TSS.1-10	A	Document the reference to the exact location(s) in the TSS.
ASE_TSS.1-11	A	Report whether an SOF level exists and whether it is one of the 3 valid levels.
ASE_TSS.1-12	C	Identify the salient characteristics of the evidence/TOE that were reviewed for completeness and provide rationale as to why the selected characteristics are sufficient.
ASE_TSS.1-13	C	Identify the salient characteristics of the TSS that were reviewed for coherency and provide rationale as to why the selected characteristics are sufficient.
ASE_TSS.1-14	C	Identify the salient characteristics of the TSS that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

EAL 4 EVALUATION

CLASS ACM: CONFIGURATION MANAGEMENT

ACM_AUT.1—Evaluation of CM Automation

Work Unit	Category	Discussion
4:ACM_AUT.1-1	A	The ETR must identify the CM Plan section that discusses the automated

		measures used to control access to the TOE implementation representation.
4:ACM_AUT.1-2	B	The ETR must describe how the automated access control measures restrict the ability to perform unauthorized changes.
4:ACM_AUT.1-3	A	The ETR must identify the CM Plan section that discusses automated generation procedures for the TOE.
4:ACM_AUT.1-4	B	The ETR should confirm that automated generation procedures can be used to ensure the correct configuration items are used in the TOE generation (e.g. UNIX makefiles under configuration management).
4:ACM_AUT.1-5	A	The ETR must identify the CM Plan section that identifies the automated tools used in the CM system.
4:ACM_AUT.1-6	B	For each tool, the evaluator should briefly describe the functionality provided by the tool and how the functionality is used to control implementation representation changes or TOE generation.
4:ACM_AUT.1-7	B	The ETR should identify how the evaluator confirmed the automated tools and procedures described in the CM plan are used (e.g. document the automated tool usage observed during a site visit).

ACM_CAP.4—Evaluation of CM capabilities

Work Unit	Category	Discussion
4:ACM_CAP.4-1	A	The ETR must include either a pointer to the relevant evidence or a reference to where the evidence is identified elsewhere in the ETR. The ETR must include the unique id for the TOE.
4:ACM_CAP.4-2	A	The ETR must show an existence decision (i.e., Y/N) and it must also identify how the labeling is accomplished (e.g., software, hardware, physical marking).
4:ACM_CAP.4-3	A	Identify all relevant materials (e.g., cite any/all labels) that were compared for consistency.
4:ACM_CAP.4-4	A	The ETR should identify the location in the CM documentation where both the configuration list and how to get it are identified. The CM documentation must identify or explain where to find the specific configuration items.
4:ACM_CAP.4-5	A	The ETR must include a specific reference to the CM plan (including a unique identification of the plan, such as version number).
4:ACM_CAP.4-6	A	The ETR must include a reference to the acceptance plan (including a unique identification of the plan, such as version number).
4:ACM_CAP.4-7	C	The ETR must identify the configuration items, point to a list of configuration items included elsewhere in the ETR, or reference the pertinent document. The ETR must describe the minimum scope of configuration items that the evaluator determined must be covered by the configuration list. Additionally, the ETR must identify all relevant materials that were reviewed to determine whether the TOE is fully covered and provide rationale as to why the selected characteristics are considered complete. Document the methodology that the evaluation team applied to ascertain the coverage.
4:ACM_CAP.4-8	B	Provide affirmation that the required information exists (Y/N). The ETR must describe evaluator's methodology & analysis and the methodology used for determining adequacy. Provide pointers to the evidence that led to the evaluator's conclusion.
4:ACM_CAP.4-9	A	The ETR must include references to the relevant material (may already be included elsewhere in the ETR, in which case a pointer is sufficient). The ETR must also describe how the evaluator determined that the configuration list uniquely identified each CI.
4:ACM_CAP.4-10	B	The ETR must identify the methods applied by the CM system (e.g., see para. 1309 of the CEM) to maintain the required integrity of the TOE

		configuration items.
4:ACM_CAP.4-11	B	Reference the documents checked. Include a description of what the evaluator did and what evidence was used to establish the confidence that the CM system was being applied.
4:ACM_CAP.4-12	C	The evaluator must identify the sample selected, and any tools used. The sample selected must be justified. At a minimum, a rationale for the sample selected must be presented. The ETR must describe how the evidence/tools were used. If interviews were conducted, the persons interviewed must be identified (name and title). The rationale for selecting the interviewees must be presented, and the results of the interviews must be available (either in the ETR, or via references to the records).
4:ACM_CAP.4-13	B	The evidence used must be referenced in the ETR. Any samplings must be justified, and the methodology for the analysis must be described. Conclusions must be justified.
4:ACM_CAP.4-14	B	ETR must describe the method used to determine effectiveness of the CM access control measures; The conclusion must be justified.
4:ACM_CAP.4-15	A	The ETR must reflect the existence of the necessary materials (i.e., Y/N determination), and reference the relevant materials.
4:ACM_CAP.4-16	B	The ETR must describe the evaluator's procedures/methodology for determining effectiveness; The evaluator's conclusions must be justified.
4:ACM_CAP.4-17	B	The ETR must reference the relevant documents, and also reference the developer's acceptance criteria. For each of the items indicated in the CEM work unit (i.e., para. 1324) the evaluator must describe how adequacy was determined.
4:ACM_CAP.4-18	B	The ETR must describe the evaluator's procedures/methodology for determining that the configuration items are identified in a way that is consistent with the CM documentation. Justify how the configuration items are uniquely identified.

ACM_SCP.2—Evaluation of CM scope

Work Unit	Category	Discussion
4:ACM_SCP.2-1	A	The ETR should identify the location of the configuration list in the CM system and justify that the list includes the minimum set of items required by the CC to be tracked by the CM system..
4:ACM_SCP.2-2	N/A	CCIMB interpretation 0004, "ACM_SCP.*.1C Requirements Unclear," deleted this work unit.

CLASS ADO: DELIVERY AND OPERATION

ADO_DEL.2—Evaluation of delivery

Work Unit	Category	Discussion
4:ADO_DEL.2-1	B	Include pointers to the delivery procedures where the following information is presented. Note that if the information identified below is not applicable, provide a justification as to its exclusion. --determine identification of TOE, -maintain integrity during transfer of TOE or component parts, --describe which parts of TOE need to be covered by these procedures, --describe physical or electronic distribution where applicable, --show confidentiality and availability concerns are considered if necessary, and --show that the procedures are applicable across all delivery phases.

4:ADO_DEL.2-2	B	Explain how the suitability analysis was performed based on the security objectives (if present) and the specific TOE.
4:ADO_DEL.2-3	B	Include pointers to the evidence where there is a description of the various procedures and technical measures used to detect modification or any discrepancy between the developer's master copy and the version received at the user site.
4:ADO_DEL.2-4	B	Include pointers to the evidence where there is a description of procedures to detect attempts of masquerading.
4:ADO_DEL.2-5	B	Describe which approach was taken and document the results.

ADO_IGS.1—Evaluation of installation, generation, and start-up

Work Unit	Category	Discussion
4:ADO_IGS.1-1	A	Include pointers to the evidence that show where the procedures for secure installation, generation, and start-up of the TOE are provided. Perform the install and document results.
4:ADO_IGS.1-2	B	Include pointers to the evidence that describe the steps necessary for secure installation, generation, and start-up of the TOE. If the procedures will or can be reapplied, (e.g., because the TOE is not delivered in an operational state) then the ETR must provide pointers to the following information within the procedures: --information about changing the installation specific security characteristics of entities under the control of the TSF --handling exceptions and problems, --minimum system requirements for secure installation, if applicable. AND The evaluator is required to follow or perform checks on the developer's procedures using the supplied guidance documentation only. The ETR should document the results of the procedure check.

CLASS ADV: DEVELOPMENT

ADV_FSP.2—Evaluation of functional specification

Work Unit	Category	Discussion
4:ADV_FSP.2-1	A	Note either that the HLD was informal (in which case this work unit is not applicable) or where the explanatory text is located.
4:ADV_FSP.2-2	C	Identify the salient characteristics of the evidence/TOE that were compared for internal consistency and provide rationale as to why the selected characteristics are sufficient.
4:ADV_FSP.2-3	C	Document how the functional specification was judged to identify all external TOE security function interfaces. Provide a rationale to demonstrate that *all* external TOE security function interfaces were identified.
4:ADV_FSP.2-4	C	Document how the functional specification was judged to describe all external TOE security function interfaces. Provide a rationale to demonstrate that all external TOE security function interfaces were described to an adequate level of detail, including the evaluator's justification for determining whether each interface is or is not security relevant.
4:ADV_FSP.2-5	C	Document how the evaluator determined that the TSF interfaces were adequately described. The ETR must include a table containing each

		TSFI and addressing each of the items identified in CEM paragraph 1379. CEM paragraph 1381 describes an iterative review comparing each TSFI presentation in the FSP with the design, source code, or other evidence. If this type of iterative review is *not* performed, the evaluator must provide a rationale for why it was omitted, including a description of what other methods were used to make the determination of adequacy and correctness of the TSFI presentation. If CEM paragraph 1381 is followed, the ETR must document in detail the comparison of each TFSI to the design, source code, or other evidence.
4:ADV_FSP.2-6	C	Document the comparison of the TSF representation to: the TSS in the ST, the user guidance, and the administrator guidance. This work unit must demonstrate that no security functions are absent from the TSF presentation in the functional specification.
4:ADV_FSP.2-7	B	Provide a pointer to the convincing argument for completeness. Describe the methodology that was used to determine that the argument was convincing.
4:ADV_FSP.2-8	B	Provide a pointer to the mapping between the functional specification and the TSS. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *completeness* of the mapping was determined.
4:ADV_FSP.2-9	B	Provide a pointer to the mapping between the functional specification and the functional requirements. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *accuracy* of the mapping was determined (i.e., demonstrate that the detailed information in the functional specification is exactly as it is specified in the ST.)

ADV_HLD.2—Evaluation of high-level design

Work Unit	Category	Discussion
4:ADV_HLD.2-1	A	Note either that the HLD was informal (in which case this work unit is not applicable) or where the explanatory text is located.
4:ADV_HLD.2-2	C	Identify the salient characteristics of the evidence/TOE that were compared for internal consistency and provide rationale as to why the selected characteristics are sufficient.
4:ADV_HLD.2-3	C	List all subsystems by name and justify why the subsystem composition is sufficient or insufficient. The justification should address the appropriateness of the subsystems and the choice of grouping of functions within those subsystems. A rule of thumb is that the subsystems are defined in terms of the functional design of the TOE and are completely independent of the actual implementation. In other words, all TOEs of a given TOE type could have identical high-level designs, despite the fact that all of the implementations are vastly different. For example, all operating systems work basically the same way; therefore they would all be expected to have the same subsystems: a process manager, a file manager, a device manager, an administrative subsystem, an authentication subsystem, an audit subsystem, etc. If the subsystems are too low-level (e.g. each source file), there will be so many that no clear picture the workings of the TOE will be provided; if they are too high-level (e.g. the entire kernel as a single subsystem), the description of its purpose will be overly complicated because it will be responsible for so much. In both of these extremes, no clear picture the workings of the TOE will be provided so no understandability of the TOE is achieved.
4:ADV_HLD.2-4	B	Note reference to the description of all the actions that each subsystem may perform through its functions and the effects each subsystem may have on the security state of the TOE. The descriptions of the

		subsystems should be sufficient so that it is clear which subsystems are involved in each of the security functions identified in the functional specification.
4:ADV_HLD.2-5	A	Give a reference to identification of the hardware/firmware/software required by the TSF.
4:ADV_HLD.2-6	B	Note reference to necessary functions of underlying hw/fw/sw. This work unit is not applicable if there are no security requirements on the IT environment.
4:ADV_HLD.2-7	A	Give a reference to the identification of the interfaces to the TSF subsystems. For each subsystem, provide a reference to the name of each of its entry points.
4:ADV_HLD.2-8	A	Give a reference to the identification of each of the interfaces to the subsystems of the TSF that are externally visible.
4:ADV_HLD.2-9	C	Justify the adequacy of the subsystem interface descriptions, taking into consideration the testing approach used to meet the ATE_DPT requirement. The justification should provide a rationale for differences in level of detail for different interfaces, if applicable.
4:ADV_HLD.2-10	A	Give a reference to the identification of which subsystems are directly or indirectly TSP-enforcing.
4:ADV_HLD.2-11	B	Provide a pointer to the mapping between the high level design and the TOE security functional requirements. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *accuracy* of the mapping was determined (i.e., demonstrate that the detailed information in the high level design is exactly as it is specified in the ST).
4:ADV_HLD.2-12	B	Provide a pointer to the mapping between the high level design and the TOE security functional requirements. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *completeness* of the mapping was determined.

ADV_IMP.1—Evaluation of implementation representation

Work Unit	Category	Discussion
4:ADV_IMP.1-1	B	Justify why the implementation representation is suitable for analysis.
4:ADV_IMP.1-2	B	Justify why the implementation representation is adequate and appropriate. Document how the principles of sampling were applied to determine the adequacy and appropriateness.
4:ADV_IMP.1-3	C	Identify the salient characteristics of the evidence/TOE that were compared for internal consistency and provide rationale as to why the selected characteristics are sufficient.
4:ADV_IMP.1-4	B	The implementation representation subset must accurately instantiate the relevant TOE security functional requirements. Document how such accuracy was determined. For SFRs that are implemented within a specific file or set of files, a simple table mapping each SFRs to the areas of code that implement it would suffice. For SFRs that are architecturally based (e.g. FPT_SEP, FPT_RVM), a textual description of how the SFRs are accomplished is required. Provide a pointer to the mapping between the implementation representation subset and functional requirements and its justification.

ADV_LLD.1—Evaluation of low-level design

Work Unit	Category	Discussion
4:ADV_LLD.1-1	A	Note either that the LLD was informal (in which case this work unit is

		not applicable) or where the explanatory text is located.
4:ADV_LLD.1-2	C	Identify the salient characteristics of the evidence/TOE that were compared for internal consistency and provide rationale as to why the selected characteristics are sufficient.
4:ADV_LLD.1-3	A	Give a reference to the location in the LLD where the all modules are clearly and unambiguously identified.
4:ADV_LLD.1-4	B	Give a reference to the description of the purpose of each module. Justify how each purpose description is clear enough to convey what functions the module is expected to perform.
4:ADV_LLD.1-5	B	Give a reference to a description of the interrelationships of each module to others with which it communicates or on which it depends.
4:ADV_LLD.1-6	C	Justify that the low level design describes *how* each TSP-enforcing function is provided. The justification must include how each description is sufficiently refined so as to permit an implementation to be created.
4:ADV_LLD.1-7	A	Give a reference to identification of all entry points for each module.
4:ADV_LLD.1-8	B	Document how the low level design was judged to identify all external interfaces to the modules of the TSF. Provide a rationale to demonstrate that *all* external TSF module interfaces were identified.
4:ADV_LLD.1-9	C	Justify the adequacy of the module interface descriptions, taking into consideration the testing approach used to meet the AVA_VLA requirements. The justification should provide a rationale for differences in level of detail for different interfaces, if applicable.
4:ADV_LLD.1-10	A	Give a reference to the identification of which modules are directly or indirectly TSP-enforcing.
4:ADV_LLD.1-11	B	Provide a pointer to the mapping between the low level design and the TOE security functional requirements. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *accuracy* of the mapping was determined (i.e., demonstrate that the detailed information in the low level design is exactly as it is specified in the ST).
4:ADV_LLD.1-12	B	Provide a pointer to the mapping between the low level design and the TOE security functional requirements. The ETR must include whether the developer provided the mapping or whether the evaluator had to construct the mapping. The ETR must justify how the *completeness* of the mapping was determined.

ADV_RCR.1—Evaluation of representation correspondence

Work Unit	Category	Discussion
4:ADV_RCR.1-1	C	Include a mapping to justify that the functional specification is a correct and complete representation of the TOE security functions.
4:ADV_RCR.1-2	C	Include a mapping to justify that the high level design is a correct and complete representation of the functional specification.
4:ADV_RCR.1-3	C	Include a mapping to justify that the low level design is a correct and complete representation of the high level design.
4:ADV_RCR.1-4	C	Include a mapping to justify that the subset of the implementation representation is a correct and complete representation of the portions of the low level design that are refined in the implementation representation.

ADV_SPM.1 Evaluation of security policy modeling

Work Unit	Category	Discussion
4:ADV_SPM.1-1	A	Note either that the model was informal (in which case this work unit is not applicable) or where the explanatory text is located.

4:ADV_SPM.1-2	A	Report where all security policies explicitly included in the ST are modeled. Note that if FDP_ACC and FDP_IFC are not included in the ST, this work unit is not applicable.
4:ADV_ SPM.1-3	B	Identify all security policies represented by the security functional requirements claimed in the ST and indicate where each such policy is modeled.
4:ADV_ SPM.1-4	B	Justify that the modeled security behavior of the TOE is *clearly* articulated.
4:ADV_ SPM.1-5	C	Describe how the consistency analysis was performed. Justify that the consistency rationale was adequate. Include all mapping tables that were constructed.
4:ADV_ SPM.1-6	C	Map the rules and characteristics of the security policy model to explicit policy statements (i.e., functional requirements). Justify the completeness of the security policy model rationale.
4:ADV_ SPM.1-7	C	Justify that all functions that directly support the security policy model have been identified and verify that these functions are present in the functional specification correspondence demonstration of the security policy model. Include any mapping tables constructed.
4:ADV_ SPM.1-8	C	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.

CLASS AGD: GUIDANCE DOCUMENTS

Some of the AGD work units use a list of relevant questions in the discussion section. For such work units, each question must be addressed in the corresponding section of the ETR. For the other AGD work units, a description of what information must be presented in the ETR is given in the discussion section.

AGD_ADM.1—Evaluation of administrator guidance

Work Unit	Category	Discussion
4:AGD_ADM.1-1	B	--Document what administrative documentation was evaluated including a description of the process used to identify that these documents (which could be fragments of documents) are administrative documentation. Consider the ST TSS, any documentation with the title "Administrator", and installation guidance. --Justify that no TOE administrative guidance was incorrectly omitted from examination (in other words, is it plausible that their process identified all necessary documentation) including a description of the process used to ensure nothing was missed (this may be a different process than the previous point). Justify that user guidance was examined to ensure there was no critical omission (sometimes administrators are assumed to have also read the user documentation, in which case the user documentation is a subset of the administrator documentation). --Document where (which documentation and section(s)) the overview of the security functionality that is visible at the administrative interface is provided. Since this would be a starting point for others, the evaluator should specifically identify this location. --Describe the process was used to determine if the administrator guidance identified and described the purpose, behavior, and interrelationships of the administrator security interfaces and functions. Justify that the

		administrative interface identifies & describes the purpose, behavior, and interrelationships of the administrative security functions and interfaces. Interrelationships are often shown by a graphic or matrix. --Document the process used to determine that for each administrator security interface and function, the administrator guidance met the CEM guidance. Document how the determination was made that the administrative guidance described the invocation method, parameters, and responses. Justify that the valid and default values of parameters were documented in the administrative guidance. A brief example/description of the documentation would be helpful, e.g., "We found that the administrative guidance followed the following documentation format {brief description showing where the various kinds of information should be found}, which if followed would provide this information. We then examined of the actual {number or some other measure of size} entries, and in each case found that they provided the CC-required information." The goal is to show that work was actually performed, and not just a simple "We determined that the documentation met CC requirements."
4:AGD_ADM.1-2	B	--Document the process used to determine this (a mapping of these functions to administrative guidance areas might be a way to do this; if expanded, this could also support AGD_ADM.1.6). Justify that the administrative guidance discusses how to securely implement all the administrative functions identifiable from the SFRs and the ST TSS. As applicable, the administrative functions should include: the start-up/power-on, shutdown/power-off, security management (FMT) functions, adding/removing accounts/roles/privileges, storing and transferring certificates/keys/passwords, and performing backups. --Justify and provide a rationale that the guidance provides sufficient information to cover an IT environment consistent with the one in the ST. If the administrative guidance covers many environments, document where it clearly states when it applies or does not apply to a situation relevant to the ST.
4:AGD_ADM.1-3	B	--Describe the process used to identify the functions and privileges that should be controlled in a secure processing environment (e.g., examining the different major services and how their privileges could be separately granted). Note that in this case, evaluating more than the administrative guidance is necessary, since the issue is completeness of the administrative guidance; especially useful sources include the ST, user guidance, and high-level design. Follow (and document the results of) the CEM guidance for identification of the evidence inputs. Document the key functions/privileges. --Document the process used to determine that administrative guidance included warnings about them. A likely process is a mapping from the functions and privileges (noted above) to the administrative guidance sections discussing them. Justify that those warnings include the information recommended by the CEM.
4:AGD_ADM.1-4	B	--Document the process used to identify the assumptions regarding user behavior. The ST TOE security environment (esp. the assumptions section) should be an especially rich source of information, but other documents (especially the user guidance and design documents) must also be examined to identify assumptions. If there is information users must keep safe (passwords, certificates, hardware tokens), this must be a documented assumption. --Justify that the administration guidance included all such information. This might be done by mapping a list of user assumptions to sections of the administrative guidance.
4:AGD_ADM.1-5	B	--Justify that the administrator guidance describes every security parameter's purpose, valid value, default value, secure settings, and insecure settings.

		Note that AGD_ADM.1.1 identified the parameters. This justification might be done as a mapping from the security management functions (FMT) plus any derived parameters to the administrative guidance, showing that they are described. Note that this action might be performed as part of AGD_ADM.1.2. --Justify that the parameter settings were examined in combination. This could be done by grouping parameters into larger groups of settings, and then developing an interaction table showing the possible interactions of the groups (self-interactions may or may not be irrelevant, depending on the system). Note that examining all combinations could rapidly become difficult in a large system, so grouping or other methods to simplify the analysis may be needed.
4:AGD_ADM.1-6	B	--Document the types of security-related events. Document the process used to derive these events. This list might be derived from examining the security functions in AGD_ADM.1.1. This should include audit trail overflow, out of resource (e.g., memory or disk), system crash, failure of a trusted program or component. --Document where administrator response is described for these events. This could be described as a mapping from the event to the documentation location. --Justify why these responses are sufficient. Clearly, just having documentation isn't enough if the documentation fails to securely respond to the event.
4:AGD_ADM.1-7	B	Justify that the administrator guidance was consistent with all other documents supplied for evaluation. In particular, describe documents were examined, and how. Ensure that the ST (especially the security environment, security objectives) was examined to identify warnings. A mapping of such warnings to administrative text describing the issues would be good evidence. Note that AGD_ADM.1.3 is similar, but not the same, as what is required here.
4:AGD_ADM.1-8	B	Justify that the administrative guidance describes all IT security requirements for the IT environment of the TOE that are relevant to the administrator. Usually, this would be done with a small table listing the IT security requirements, and mapping them to sections of the administrative guidance. In cases where no administrator guidance is appropriate, or where the mapping might not be clear, a comment should be made to that effect justifying that conclusion.

AGD_USR.1—Evaluation of user guidance

Work Unit	Category	Discussion
4:AGD_USR.1-1	B	--This CEM work unit for CC element AGD_USR.1.1C is a fairly straightforward example of verifying the existence and completeness of system documentation. The CEM is clear that the user guidance must adequately cover an overview of the security functionality that is visible at the user interface. To demonstrate that, some correlation must be determined between the system documents that describe the untrusted user interface and the topics contained in the non-administrative user guidance documents. A simple comparison of interface identifiers to user document descriptions should be sufficient for demonstrative compliance. ETR descriptions must document compliance determination by identifying relevant evaluation documents and stating that a successful comparison was conducted along with a description of the process used, and a table showing the comparison. --For this work unit the CEM also requires that the user documentation must identify the purpose and functions of security interfaces. The CEM language

		is equally clear here in that the documentation for each non-administrative interface must be examined, by the evaluator, and found to include an explanation of its purpose and functions. Simple ETR statements of this fact should be sufficient.
4:AGD_USR.1-2	B	The CEM language for this work unit is very clear on what must be verified, by the evaluator, when inspecting user guidance descriptions of security functions. That is, the behavior and interrelationships must be clearly described. Any special sequence ordering of command execution must be accounted for as well as the actions that any command could have. The user guides containing this information must be cited and statements made that evaluators examined each identified and documented interface. All TOE user accessible interfaces must be explicitly examined. Likewise the CEM language concerning determination of the methods by which interfaces are invoked, existence and effects of parameters defined for each interface, and TSF responses, messages, or error codes, is complete. Evaluator actions to verify this can be varied but would most likely use the results of any comparison developed for AGD_USR.1-1. ETR sections must describe how all the relevant features of the identified interfaces were examined as well as the documents referenced.
4:AGD_USR.1-3	B	--The CEM is very comprehensive regarding what elements of interfaces need to be described in the user guidance regarding the use of privileges or additional capabilities that could be gained by users. Evaluators need to review user guidance documents and verify that all the possible interface elements or capabilities are described for all identified interfaces and how the privileges that can be used are controlled. In particular any warnings about the effects of interface actions must be covered. --ETR sections that account for the referencing of the ST and functional specifications, by the evaluator, for specifics about the operating environment would suffice.
4:AGD_USR.1-4	B	--The CEM is quite explicit in pointing out that evaluators need to review all user guidance information concerning any assumptions about user behavior. This may entail reviewing numerous documents, possibly including the ST. Plus assumptions can occur in two forms: explicit and implicit. Implicit assumptions are more subjective to identify and would require greater care in their identification. --ETR sections should include information concerning identification of the documents that were considered, by the evaluators, as well as the process that was used to identify explicit, and especially, implicit assumptions. --This CEM work unit also calls for the identification of advice to users regarding the effective user of security functions. It mentions examples such as protecting user passwords. This is a very open-ended activity since providing “adequate” advice on the use of the TOE lacks any sort of firm metric. In satisfying this requirement, and documenting it in the ETR, the evaluator must describe their approach to establishing an acceptable level of amount of advice (e.g., one piece of advice/security function, advice given only for a select and identified group of security functions) presented. --Lastly, the CEM points out that user documentation should indicate whether functions can be invoked directly by users or whether they require administrative assistance. To answer this question evaluators can do a simple review of all documented functions and verify that operations that obviously require administrative assistance. ETR descriptions can simply describe the process and report that it was followed.
4:AGD_USR.1-5	B	--Here the CEM requires the evaluator to examine all other documents supplied for evaluation to ensure that the information in them does not contradict the user guidance. In particular, the ST is called out for attention lest it contain warnings to users about the security environment or security

		objectives; such warnings must be consistent with user guidance. --ETR sections for this work unit should list the documents examined, note any descriptions of requirements on or warnings to the user, and call out any inconsistencies found.
4:AGD_USR.1-6	B	--If the ST contains security requirements for the IT environment, the CEM requires the evaluator to select any such requirements that relate to the user, and then to ensure that these user-relevant IT security requirements are described appropriately in the user guidance. --The ETR sections should refer to the requirements in the ST for the IT environment that relate to the user, and the sections of the user guidance where these requirements are discussed.

CLASS ALC: LIFE CYCLE SUPPORT

ALC_DVS.1—Evaluation of development security

Work Unit	Category	Discussion
4:ALC_DVS.1-1	B	The CEM is reasonably clear in describing this evaluator activity. The evaluator is expected to determine the security measures that are necessary for the protection and integrity of the TOE design and implementation and then to confirm that each of those measures is adequately detailed in the security documentation. The evaluator records should be sufficient to determine the actions that were performed to complete this activity as well as to capture the results of the activity in the ETR. The results of this activity should be documented in the ETR in sufficient detail that without referring to other documentation the reader could compose a list of all of the security measures that the evaluators determined were necessary and the associated locations in the security documentation where the details of each of those security measures can be found.
4:ALC_DVS.1-2	B	The ETR documentation for this activity should provide the reader with a description of the analysis that was performed to determine the sufficiency of the security measured employed. The reader should have sufficient information to be able to construct from the ETR rationale a listing of the appropriate policies, a documentation cross-reference of where those policies are described, and a description of the analysis of the security measures employed that is sufficient to support the conclusion that the measures are complete and consistent. The ETR should specify the criteria that the evaluators used to determine that the measures were complete and consistent. The rationale could make reference to further evaluation records that detailed the completeness and consistency analysis and actually documented that each of the criteria was met.
4:ALC_DVS.1-3	B	--The CEM does not provide much detailed guidance on this activity other than a reference to the general guidance on sampling. --The evaluators should document in the ETR the sample of specific applications of the procedures and associated documentary evidence that the evaluators chose to check, their rationale for selecting that set of procedures and evidence as a representative sample, the documentary evidence that the evaluators expected to find when the check was performed, and method that the evaluators used to keep track of their conclusions as each of the sample items in the documentary evidence was checked for compliance with the associated procedures. The documentary evidence that the evaluators expected to find may be characterized in the ETR with the details of the checking (specific evidence identifiers, etc) being documented in evaluation records that are referenced in the ETR.
4:ALC_DVS.1-4	B	--The ETR needs to contain enough detail about the manner in which this

		activity was performed that a reader can determine for each security measure that was identified in activity ALC_DVS.1-4 which security documentation and associated evidence was examined to determine that the specific security measure was being applied. --The CEM provides guidance for this activity that strongly encourages that a site visit be performed in conjunction with this activity. However, a site visit is not necessary and the evaluators may make their determination through other means. In the case where a site visit was involved, the ETR should explain the role of the site visit in the performance of this evaluator action. In a case for which a site visit was not performed, the ETR should explain the manner in which it was determined that the physical measures were being applied and the development staff was aware of the development security policies and procedures and their responsibilities.

ALC_LCD.1—Evaluation of life-cycle definition

Work Unit	Category	Discussion
4:ALC_LCD.1-1	B	The CEM gives a reasonably complete description of the information that it expects an evaluator look for when examining the life-cycle documentation. In particular, it expects the evaluator to look for the appropriate tools, techniques, procedures, and management structure to be described in the documentation. Although the evaluators do not need to provide an overview of the life-cycle model in the ETR, the ETR should state the criteria that the evaluators used to determine whether the life-cycle model covered the development and maintenance process, the method that the evaluators used to determine that it was covered, and evidence (or reference to further evaluation records) showing that the evaluators found that each aspect was (was not) covered. This description should be detailed enough that a reader could single out each significant component of the development and maintenance process and determine the associated pieces of the life-cycle model description that covered it.
4:ALC_LCD.1-2	B	The CEM does not provide very good guidance for this evaluator action. The CEM states that almost any life-cycle model could be deemed adequate under the appropriate circumstances. The evaluators should document in the ETR the identification of the "necessary contribution," a criteria for determining when it has been met, and an explanation of why the use of the tools, techniques, procedures etc. ensure that the criteria is met. Although the CEM discusses the "necessary contribution" in terms of the likelihood of introduction of flaws into the TOE, the CEM does not provide much useful guidance in determining the "necessary contribution". Most of the specific aspects of the development and maintenance process that reduce the likelihood of the introduction of flaws into the TOE will also be covered by other CC requirement – design, testing, configuration management, vulnerability analysis, tools and techniques, flaw remediation, etc. Hence, the rationale that covers this evaluator action and the associated ETR text may refer the reader to the ETR sections for those other components of the development and maintenance process for much of the evidence that the "necessary contribution" is provided.

ALC_TAT.1—Evaluation of tools and techniques

Work Unit	Category	Discussion
4:ALC_TAT.1-1	C	1. The evaluator must determine whether the language has an accepted standard definition or is proprietary. If proprietary, the evaluator must determine whether the language meets the definition of well-defined in the CEM: "a clear and complete description of its syntax, and a detailed

		description of the semantics of each construct." If a standard language, ask: --Does the documentation assert conformance with the standard? --Does the documentation identify any deviations from the standard: Constructs in the standard with non-standard or extended meanings? Constructs not in the standard? If so, are the deviations and extensions clearly defined? 2. The evaluator should determine the source and version of the compiler. Although the CEM does not specifically call this out, it is necessary to assess the trustworthiness of the compiler and to identify any version-related flaws that might be known or discovered. Note that a developer may choose not to use the branded compiler from the vendor of the development platform. 3. The CEM is very clear about the purpose of this sub-activity: "The critical test is whether the evaluator can understand the TOE source code when performing source code analysis covered in the ADV_IMP sub-activity." "The evaluator should verify, during the examination of source code, that any use of the problematic constructs does not introduce vulnerabilities. The evaluator should also ensure that constructs precluded by the documented standard are not used." The result of ALC_TAT is to demonstrate that the documentation enables the evaluator to understand the source code sufficiently to support the evaluator's judgment as to the sufficiency and correctness of the code sample examined in ADV_IMP. ***ALC_TAT.1.1C Example: Evaluator Actions*** The evaluator ascertained that the developer's software is written in a combination of C language and assembly language for the IBM PC with an Intel Pentium 4 CPU. The developer uses: --Tower C compiler, ver. 1.12, from XIM Software Tower C claims conformance with ISO/ANSI C (ISO/IEC 9899:1999 and the C Corrigendum, ISO/IEC 9899/Cor1:2001), with the following extensions: *<Insert list of extended constructs and their definitions here, or list them in another location pointed to from here.>* --X86 Assembler ver. 4.79 from I. Ericson Software. The Ericson compiler claims conformance with the programming specifications in the IA-32 Intel® Architecture Software Developer's Manual, Intel Order Numbers 245470-008, 245471-008, and 245472-008. The evaluator examined the Power C Programmer's Manual and determined that the language description in the manual, excluding the proprietary extensions, conforms to the ISO/ANSI standard. The evaluator examined the documented syntax and semantics of each non-standard language extension to assess its clarity and completeness. The evaluator examined the Ericson X86 Assembler Manual and determined that the language description in the manual mapped completely and unambiguously to the instruction set, register usage, procedure calls, interrupts, and exceptions in the x86 subset of the IA-32 Intel® Architecture Software Developer's Manual.
4:ALC_TAT.1-2	C	The CEM identifies some common areas of ambiguity or uncertainty in programming language documentation. The evaluator must identify all such problems in the development tool documentation and ensure that code in the examined subset of the implementation representation does not contain any dependencies on problematic constructs.

		ALC_TAT.1.2C Example: Evaluator Actions The evaluator examined the Power C Programmer's Manual and determined that the following extensions were not adequately explained: --The definition of the non-standard function *mumble(x,y)* refers to the division of an intermediate result by *sin(y)* but says nothing about the value of the function when *y=0*. -- … < Insert list of other problematic extensions and non-standard constructs.> The evaluator examined the A386 Assembler Manual and found no deviations from the Intel® Architecture Software Developer's Manual. Once the evaluator has identified problematic extensions and non-standard constructs in the programming language documentation, the evaluator must also examine the subset of the implementation representation to ensure that it does not use these extensions or non-standard constructs, as specified by CEM paragraphs 1560 and 1561.
4:ALC_TAT.1-3	C	Implementation-dependent options include compiler switches that control aspects of the compilation process, macro constructs such as "#define" in C, source text inclusion operators such as "#include" in C, conditional preprocessing or compilation operators such as "#if" in C, etc. ***ALC_TAT.1.3C Example: Evaluator Actions*** The evaluator examined the compiler and assembler macro definitions and C *#include* files used by the developer in compiling/assembling the components of the TOE. Their names and functions are shown in Table 3. All were found to be clearly readable and unambiguous. Nesting of definitions was shallow and easily traced. The evaluator examined the compiler, assembler, and linker control options used by the developer in building the TOE. All are clearly defined in the respective vendors' documentation. Each tool's options and their meanings are shown in Table 4.

CLASS ATE: TESTS

ATE_COV.2—Evaluation of coverage

Work Unit	Category	Discussion
4:ATE_COV.2-1	B	Justify the accuracy of the correspondence between the tests identified in the test documentation and the functional specification.
4:ATE_COV.2-2	B	Justify the suitability of the testing approach for each security function of the TSF to demonstrate the expected behavior.
4:ATE_COV.2-3	B	Justify the adequacy of the test prerequisites, test steps and expected result(s) to test each security function.
4:ATE_COV.2-4	B	Provide a mapping between the TSF as described in the functional specification and the tests identified in the test documentation to justify completeness of the test coverage.

ATE_DPT.1—Evaluation of depth

Work Unit	Category	Discussion
4:ATE_DPT.1-1	B	Justify that the mapping (and rationale, if necessary) between the tests identified in the test documentation and all the subsystems described in the high-level design is sufficient to show test correspondence.

4:ATE_DPT.1-2	B	Justify that the testing approach for each security function of the TSF is suitable to demonstrate the expected behavior. The justification must include a discussion of whether testing of the TSF was performed at the external interfaces, internal interfaces, or a combination of both and why the chosen testing method was suitable.
4:ATE_DPT.1-3	B	Justify the adequacy of the test prerequisites, test steps and expected result(s) to test each security function.
4:ATE_DPT.1-4	B	Justify the completeness of the mapping between the TSF as defined in the high-level design and the tests in the test documentation.

ATE_FUN.1—Evaluation of functional tests

Work Unit	Category	Discussion
4:ATE_FUN.1-1	A	Provide pointers to the location of the required information in the test documentation.
4:ATE_FUN.1-2	B	Justify that the security functions to be tested are identified in the test plan, citing specific references to the functional specification.
4:ATE_FUN.1-3	B	Justify that the test plan provides information about how the security functions are tested and the test configuration(s) in which testing occurs.
4:ATE_FUN.1-4	B	Justify how the determination was made that the TOE test configuration is consistent with the configuration identified for evaluation in the ST. If more than one model is included in the evaluation, include a rationale for why the test configuration is representative of all models defined in the ST.
4:ATE_FUN.1-5	B	Provide a justification as to how the determination was made that the test plan is consistent with the test procedure descriptions.
4:ATE_FUN.1-6	B	Justify that the security function behaviors to be tested are identified in the test procedure descriptions, citing specific references to the design specification.
4:ATE_FUN.1-7	B	Justify that the test procedure descriptions are sufficient to establish reproducible initial test conditions including ordering dependencies if any.
4:ATE_FUN.1-8	B	Justify that the test procedure descriptions provide sufficient instructions to have a reproducible means to stimulate the security functions and to observe their behavior.
4:ATE_FUN.1-9	B	Provide a table to justify that the test procedure descriptions are consistent with the test procedures (if applicable).
4:ATE_FUN.1-10	B	Justify the sufficiency of the expected test results, including how the test results are unambiguous and consistent with expected behavior.
4:ATE_FUN.1-11	C	Actual test results reported must provide meaningful information including a description of the result of the test (i.e., a reported result of "pass" or "fail" is inadequate). If data reduction or synthesis of the actual test results is performed, justify that the process used by the developer is correct. Justify consistency between actual and expected test results.
4:ATE_FUN.1-12	C	Report the developer testing effort, outlining the testing approach, configuration, depth and results. The report should be written with enough detail to allow the validator to gain insight into the technical quality of the testing effort in order to make a determination of sufficiency and correctness.

ATE_IND.2—Evaluation of independent testing

Work Unit	Category	Discussion
4:ATE_IND.2-1	B	Justify how the determination was made that the TOE test configuration is consistent with the configuration identified for evaluation in the ST. If more than one model is included in the evaluation, include a rationale for why the test configuration is representative of all models defined in the ST. A reference to a developer-provided justification or mapping may be included as part of the justification.
4:ATE_IND.2-2	B	Install the TOE and document the results to provide justification that the TOE is installed properly and is in a known state. If the evaluator does not perform the actual installation, then a justification of how the developer has met the requirement must be provided.
4:ATE_IND.2-3	C	Provide a justification that the set of resources provided by the developer is equivalent to the set of resources used by the developer to functionally test the TSF.
4:ATE_IND.2-4	C	Provide a justification for test subset selection and testing strategy. The justification must address CEM paragraphs 1642-1647.
4:ATE_IND.2-5	C	The detailed test documentation produced for the test subset should demonstrate an understanding of the expected behavior of the security functions.
4:ATE_IND.2-6	C	All test documentation developed for independent testing should be used. Any additional ad hoc tests must be documented to the same level of detail as the planned tests.
4:ATE_IND.2-7	B	Include the required information for the tests that compose the test subset, per the CEM.
4:ATE_IND.2-8	A	Justify that all the actual test results are consistent with the expected test results.
4:ATE_IND.2-9	B	Justify the test sample selected and provide evidence that the testing was conducted.
4:ATE_IND.2-10	A	Justify that all the actual test results are consistent with the expected test results.
4:ATE_IND.2-11	C	The report should be written with enough detail to allow the validator to gain insight into the technical quality of the testing effort in order to make a determination of sufficiency and correctness.

CLASS AVA: VULNERABILITY ASSESSMENT

AVA_MSU.2—Evaluation of misuse

Work Unit	Category	Discussion
4:AVA_MSU.2-1	B	Cite applicable documents, including document version numbers, since version numbers might change as the evaluation proceeds. Justify that all the properties described in relevant paragraphs of the CEM are met and document the process used to ensure that all possible modes were covered.
4:AVA_MSU.2-2	B	Justify why the guidance is considered clear and internally consistent. Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
4:AVA_MSU.2-3	B	Justify why the guidance is considered complete and reasonable.

4:AVA_MSU.2-4	B	Document where each assumption about the intended environment is articulated.
4:AVA_MSU.2-5	B	Document where each requirement for external security measures is articulated.
4:AVA_MSU.2-6	B	Justify the completeness of the guidance, based on examination of the developer's analysis. The justification should include consideration of any deficiencies found during the conduct of work units AVA_MSU.2-1 through 2-5, and AVA_MSU.2-7.
4:AVA_MSU.2-7	B	Document the actions performed and the results obtained.
4:AVA_MSU.2-8	B	Document the actions performed and the results obtained. Justify the other guidance sampled and the approach employed.
4:AVA_MSU.2-9	C	Identify the salient characteristics of the guidance that were examined and provide rationale as to why the guidance is sufficient.
4:AVA_MSU.2-10	B	Document the actions performed. Justify that guidance is provided for secure operation in all possible modes of operation of the TOE.

AVA_SOF.1—Evaluation of strength of TOE security functions

Work Unit	Category	Discussion
4:AVA_SOF.1-1	A	Reference the SOF analysis for each security mechanism for which there is a SOF claim in the ST expressed as a SOF rating.
4:AVA_SOF.1-2	A	Reference the SOF analysis for each security mechanism for which there is a SOF claim in the ST expressed as a metric.
4:AVA_SOF.1-3	B	Justify the validity of all assertions or assumptions supporting the analysis.
4:AVA_SOF.1-4	B	Justify the correctness of all algorithms, principles, properties and calculations supporting the analysis.
4:AVA_SOF.1-5	B	Justify how each SOF claim is met or exceeded.
4:AVA_SOF.1-6	B	Justify that all functions with a SOF claim meet the minimum strength level defined in the ST.
4:AVA_SOF.1-7	C	Justify that all probabilistic or permutational mechanisms have a SOF claim. The evaluator shall examine the functional specification, the high-level design, the low-level design, the user guidance and the administrator guidance to determine that all.
4:AVA_SOF.1-8	B	Justify the correctness of each SOF claim, including documentation of any testing or independent analysis performed.

AVA_VLA.2—Evaluation of vulnerability analysis

Work Unit	Category	Discussion
4:AVA_VLA.2-1	C	Justify that the developer's search for vulnerabilities has considered all relevant information.
4:AVA_VLA.2-2	B	The evaluator shall examine the developer's vulnerability analysis to determine that each identified vulnerability is described and that a rationale is given for why it is not exploitable in the intended environment for the TOE.
4:AVA_VLA.2-3	B	Identify the salient characteristics of the evidence/TOE that were compared for consistency and provide rationale as to why the selected characteristics are sufficient.
4:AVA_VLA.2-4	C	Provide a justification for the tests derived and for the testing strategy. The justification must address CEM paragraphs 1726-1729.
4:AVA_VLA.2-5	C	The detailed test documentation produced for the penetration tests should demonstrate an understanding of the developer's vulnerability analysis and must be detailed enough to be repeatable.

4:AVA_VLA.2-6	C	All test documentation developed for penetration testing should be used. Any additional ad hoc tests must be documented to the same level of detail as the planned tests.
4:AVA_VLA.2-7	B	Actual test results reported must provide meaningful information including a description of the result of the test (i.e., a reported result of "pass" or "fail" is inadequate). Actual and expected results should be identical. Justify any differences.
4:AVA_VLA.2-8	C	The report should be written with enough detail to allow the validator to gain insight into the technical quality of the testing effort in order to make a determination of sufficiency and correctness.
4:AVA_VLA.2-9	C	This work unit must address CEM paragraphs 1736-1748. Justify the adequacy of the examination of all inputs to this subactivity in determining possible security vulnerabilities.
4:AVA_VLA.2-10	C	Justify the methodology used to devise penetration tests.
4:AVA_VLA.2-11	C	The detailed test documentation produced for the penetration tests should demonstrate an understanding of the independent vulnerability analysis and must be detailed enough to be repeatable.
4:AVA_VLA.2-12	C	All test documentation developed for penetration testing should be used. Any additional ad hoc tests must be documented to the same level of detail as the planned tests.
4:AVA_VLA.2-13	B	Actual and expected results should be identical. Justify any differences.
4:AVA_VLA.2-14	C	The report should be written with enough detail to allow the validator to gain insight into the technical quality of the testing effort in order to make a determination of sufficiency and correctness.
4:AVA_VLA.2-15	B	Justify that the TOE, in its intended environment, is resistant to an attacker possessing a low attack potential.
4:AVA_VLA.2-16	B	The ETR must be detailed enough to clearly identify and describe all exploitable and residual vulnerabilities.